LAS MATEMÁTICAS DE LA SEGURIDAD

ARBOR Ciencia, Pensamiento y Cultura
CLXXXIII 725 mayo-junio (2007) 419-425 ISSN: 0210-1963

Universidad de Oviedo

ABSTRACT: *The aim of this paper is to show the important role that Mathematics play in the Information theory. It has been intended for non specialists, drawing a general picture of the present situation.*

KEY WORDS: *Error correcting codes, cryptography, digital information, public key, secret key.*

RESUMEN: El objetivo del trabajo es mostrar el papel esencial que juegan actualmente las matemáticas en la teoría de la información. El trabajo está pensado para no especialistas y pretende dibujar en unas breves pinceladas como es la situación actual.

PALABRAS CLAVE: Códigos correctores de errores, criptografía, información digital, clave pública, clave secreta.

1. Introducción

La información, tanto por la cantidad como por la velocidad con la que circula, se ha convertido en una seña de identidad del momento actual. El trabajo de Shannon, en el que se da carácter matemático a la información, convirtiéndola en algo que se puede medir y tratar de modo científico, representó, sin lugar a dudas, un punto de inflexión en la teoría de la información. Hoy en día nadie duda de que la información es poder y como tal, un bien valioso que tiene que ser protegido de ataques a su integridad o a su confidencialidad.

Si lo pensamos detenidamente, la cantidad de información, en muchos casos información muy sensible, que circula actualmente por canales más o menos públicos, puede hacernos sentir vértigo. La mayoría de nosotros entra de modo habitual en Internet y sabe que se puede encontrar información sobre prácticamente todo, si uno sabe buscarla. Tambien estamos acostumbrados a intercambiar información con nuestro banco, con una agencia de viajes o realizando compras a través de la red. Es claro que todos nosotros deseamos tener la seguridad de que la información que enviamos sólo es accesible para su legítimo receptor y que no cae en "manos indebidas".

La seguridad de la información ha pasado de ser exclusividad de la Política, la Diplomacia, los Servicios de Inteligencia o las Altas Finanzas, a convertirse en algo cotidiano, que en mayor o menor medida nos afecta a todos y cada uno de nosotros.

Parece claro que la información tiene que ser protegida, tanto en los aspectos de fidelidad de la información, detectando y corrigiendo los posibles errores generados por el ruido (nombre genérico para todas las perturbaciones eléctricas, magnéticas o de cualquier tipo que afecten al canal por el que se transmite la información) como en el aspecto de confidencialidad e integridad de la misma. Y en este punto las Matemáticas juegan un papel de extraordinaria importancia. Siguiendo a N. Koblitz podemos decir que: "La enorme utilidad de las matemáticas en la seguridad de la información está bordeando el misterio y no existe explicación racional para ella", parafraseando a Eugene Wigner que escribió esa afirmación en relación al papel jugado por las matemáticas en las Ciencias Naturales y especialmente en Física.

2. Corrección de errores

Cuando hablamos de información siempre tenemos en mente información digital, secuencias de ceros y unos, que pueden ser transmitidos por un canal. La información de un periódico o de una fotografía no es digital, pero se puede transformar en información digital y por eso podemos leer el periódico por internet o enviar fotografías por correo electrónico. Los códigos se inventaron para corregir los errores que se producen en la comunicación a través de canales con ruido. Tratan de reproducir lo que hacemos en la vida cotidiana cuando estamos hablando y un ruido ambiental nos impide entender lo que nos ha dicho nuestro interlocutor. Le pedimos que nos repita lo que ha dicho. Por eso el primer paso es la detección de los errores en la información recibida. Pero no siempre podemos solicitar que nos reenvíen la información que ha llegado defectuosa. Aparte del coste que tiene el uso del canal, puede ser inviable. Pensemos en información almacenada en un disco y que se abre al cabo de un tiempo, cuando ya no se puede pensar en su reenvio. O en una fotografía enviada por un satélite espacial desde una posición concreta. La idea es sencilla. Se añade a la información que se quiere enviar una serie de dígitos (de control) que no contienen información, pero permiten detectar y, eventualmente corregir, errores, siempre que el número de errores producidos no exceda la capacidad correctora del código. Los códigos correctores forman parte de nuestra vida cotidiana, como ocurre con la letra que se añade al DNI o el ISBN de los libros. También lo utiliza la naturaleza en el código genético, aunque no sepamos exactamente como funciona.

En el diseño de códigos correctores de errores cuyo almacenamiento no desborde las capacidades de nuestro ordenador, las matemáticas juegan un papel decisivo. Todos los códigos considerados de modo usual son códigos lineales, es decir, disponemos de todas las herramientas del álgebra lineal. Pero no son las únicas. Teoría de cuerpos finitos, polinomios sobre ellos, geometría algebraica o matemática discreta (diseños, geometrías finitas, etc.), teoría de anillos, son algunas de las partes de las matemáticas que juegan un papel importante en la teoría de códigos correctores de errores. Dado que en general no existen algoritmos eficientes para la descodificación de un código lineal, el diseño de códigos con buenas propiedades, es decir con algoritmos de descodificación eficientes, sigue siendo un campo abierto al trabajo y la imaginación de los matemáticos, que pueden aplicar las técnicas y herramientas que les son familiares; probablemente en algunos casos de modo sorprendente.

3. Seguridad

Pero nuestro objetivo es poner de relieve el papel que juegan las matemáticas en la seguridad de la información.

La protección de la información, o más concretamente de cierto tipo de información, ha sido una preocupación de la humanidad desde tiempos remotos. Todos hemos oido hablar del cifrado usado por César para enviar sus mensajes o del escítalo de los lacedemonios. En algunos casos los procesos de cifrado fueron especialmente eficaces. Pensemos en los jeroglíficos usados por los sacerdotes egipcios, que no fueron descifrados hasta el siglo XIX. Todos estos cifrados, usados desde la antigüedad corresponden a lo que hoy llamamos criptografía de clave privada o simétrica. El texto se enmascara, transformándolo en un texto cifrado, usando para ello una clave que debe permanecer secreta y debe ser conocida sólamente por el remitente (o emisor) del mensaje y su legítimo receptor, que básicamente utiliza la misma clave para recuperar el mensaje original, o en todo caso, el coste computacional de cifrar y descifrar un mensaje es el mismo.

La auténtica revolución que cambió el panorama de la criptografía se produjo en el año 74, con el artículo en el que Diffe y Hellman introducen la criptografía de clave pública. La idea base es que la clave de cifrado de un determinado usuario A sea pública y cualquier otro usuario de la red le pueda enviar mensajes cifrados a A usando dicha clave pública. Pero sólo A, que tiene la clave privada, será capaz de descifrar los mensajes cifrados. ¿Cómo es posible que cualquier usuario pueda cifrar mensajes y no pueda descifrarlos? Es en este punto dónde las matemáticas juegan un papel esencial. La existencia de criptografía de clave pública se basa en la existencia de funciones de una vía.

Una función de una vía es una función para la cual es fácil calcular la imagen de cualquier elemento, pero la determinación de la imagen inversa de un elemento, aún sabiendo que exista, es muy costoso computacionalmente, de hecho inasumible.

Los criptosistemas de clave pública más usuales se basan en el problema de la factorización (RSA) y en el problema del logaritmo discreto. Dados dos números primos, aunque sean muy grandes, se pueden multiplicar sin problemas, pero factorizar un número grande (pensemos en números de 200 cifras decimales), aún sabiendo que es compuesto, es extremadamente costoso y requiere un tiempo que no lo hace factible. Para diseñar un esquema RSA el usuario debe elegir dos primos grandes p y q (para garantizar la seguridad p y q deben cumplir algunas propiedades adicionales) y un cierto entero e, que también veremos debe cumplir alguna condición. Su clave pública será el par (N, e) dónde $N = pq$. De este modo, los mensajes, que se identifican previamente con clases de restos módulo N (o si se quiere con enteros positivos menores que N), se cifran haciendo una exponenciación modular. Es decir, el cifrado de un mensaje m es el resto de dividir m^e entre N. Notemos que para descifrar necesitariamos hallar la inversa de la exponenciación anterior módulo N, lo que en general no se puede hacer si no se dispone de una información adicional, de la que dispone el propietario de la clave y que debe evitar llegue a ser conocida. En este caso dicha información adicional es el par de números primos p y q en los que se factoriza N.

Dado un entero n mayor que 1, se llama función de Euler de n, $\phi(n)$, al número de enteros positivos, menores que n y relativamente primos con n. Si tratamos de calcular la función de Euler de un número grande n, el procedimiento es muy costoso computacionalmente, comparable al coste de factorizar el número n. Pero si conocemos *a priori* la factorización de n, entonces es inmediato calcular $\phi(n)$. En nuestro caso, si $N = pq$, entonces $\phi(N) = (p - 1)(q - 1)$. Tambien probó Euler (del que se conmemora este año el 300 aniversario de su nacimiento) que si a es un entero relativamente primo con N, entonces la potencia $\phi(N)$ de a es congruente con 1 módulo N ($a^{\phi(N)} \equiv 1 \bmod N$). Si elegimos el entero e relativamente primo con $\phi(N)$, entonces podemos encontrar muy fácilmente, usando el algoritmo euclídeo de la división, otro entero d tal que $ed \equiv 1 \bmod \phi(N)$. Ahora para el propietario de la clave es muy fácil descifrar. Para recuperar el mensaje m cuyo texto cifrado es c ($c \equiv m^e \bmod N$) sólo tiene que hacer una nueva exponenciación, $m \equiv c^d \bmod N$.

Son resultados de teoría de números los que suministran la función de una vía en la que se sustenta la seguridad del RSA.

Otra función de una vía viene asociada al problema del logaritmo discreto. Si $G = < g >$ es un grupo cíclico convenientemente elegido, es computacionalmente imposible encontrar, para un elemento arbitrario y del grupo, el exponente x tal que $y = g^x$. Tal exponente x se llama el logaritmo discreto de y en base g. En particular se sabe que ese es el caso si tomamos como grupo cíclico el grupo multiplicativo de los elementos no nulos de un cuerpo finito (suficientemente grande) o el grupo asociado a una *buena* curva elíptica.

En este caso, si un usuario A quiere diseñar un criptosistema de clave pública tipo ElGamal, selecciona un adecuado grupo cíclico $G = < g >$, que hace público al igual que el generador del mismo y también hace público un elemento del grupo, y con $y = g^k$, siendo k un número adecuado que debe mantener secreto, difícil de determinar para cualquier otro usuario y que permitirá a A descifrar los mensajes que le envian. Notemos que k es el logaritmo discreto de y en base g, luego la seguridad del sistema se basa en que sea computacionalmente imposible calcularlo. Ahora los mensajes se identifican de algún modo con elementos del grupo. Para cifrar el mensaje m, otro usuario B determina aleatoriamente un r y envia el par (g^r, my^r). Para descifrar el mensaje, A considera la primera componente del par, g^r y la eleva a su clave privada k. Como $(g^r)^k = (g^k)^r = y^r$, para recuperar el mensaje m basta que divida la segunda componente del par recibido por el elemento $(g^r)^k$ que acaba de calcular. Notemos que r tambien debe elegirse de modo adecuado, pues un tercer usuario podría recuperar el mensaje concreto m si es capaz de determinar r que es el logaritmo discreto en base g de la primera componente del mensaje cifrado.

4. Otros tipos de criptografía

Hay otras muchas partes de las matemáticas que tienen aplicaciones en Criptografía. Por ejemplo la Combinatoria. En el año 78 se recibió con entusiasmo una propuesta de Hellman y Merkle de un criptosistema basado en el problema de la mochila. El problema de la mochila consiste en, dada una sucesión de números $\{b_1, ..., b_n\}$ y un número S (menor o igual que la suma de los términos de la sucesión) determinar si es posible encontrar algunos términos de la sucesión cuya suma

nos dé el número *S*. Se sabe que en general es un problema difícil y no existe ningún algoritmo eficiente para resolverlo (en términos de teoría de la complejidad es un problema NP-completo). Pero existe un caso en el que el problema es especialmente sencillo de resolver, las llamadas sucesiones supercrecientes, en que cada término es mayor que la suma de los que le preceden. Por ello se parte de una sucesión supercreciente, que forma parte de la clave secreta, y se enmascara con una serie de operaciones algebraicas, que tambien deben mantenerse secretas, para transformarla en una sucesión aparentemente arbitraria y sin "buenas propiedades", que es la clave pública. El recuperar el mensaje enviado a partir de su texto cifrado obligaría a un usuario no autorizado a resolver el problema de la mochila en un caso difícil, mientras que el propietario de la clave lo transforma, deshaciendo las operaciones algebraicas de su clave secreta, en un problema de la mochila en el caso sencillo de sucesiones supercrecientes, para las cuales existe un algoritmo muy eficaz.

Este esquema de cifrado y descifrado era muy eficiente, unas 100 veces más rápido que el RSA. Pero en 1984 Shamir, uno de los padres del RSA, rompió completamente el criptosistema, sin recuperar la clave secreta, sino encontrando nuevos elementos que jugaban un papel análogo y le permitian recuperar el mensaje en claro sin conocer la clave secreta. Aunque se intentó salvar el criptosistema, introduciendo iteraciones y modificaciones, todas ellas fueron rotas por Shamir. Durante un tiempo se consideró que la criptografía basada en problemas combinatorios no tenia futuro, a pesar de la existencia de muchos problemas NP-completos conocidos que serian los candidatos naturales para definir una función de una vía. No obstante hoy en día se ha recuperado la idea de utilizar problemas de combinatoria y se está produciendo una notable actividad en esta dirección, si bien no hay todavía ninguna propuesta concreta que sea viable y eficaz.

La aparición de los ordenadores cuánticos supondria una amenaza letal para los sistemas criptográficos de clave pública más utilizados (basados en factorización y en el problema del logaritmos discreto), dado que el proceso de multiplicar dos números y la factorización de un número pasarian a ser problemas de complejidad similar con un ordenador cuántico. Por ello se han buscado primitivas criptográficas basadas en otros aspectos matemáticos, con problemas en los que un ordenador cuántico no supondría un cambio sensible. Una de las ramas que ha jugado y juega un papel fundamental es la teoría de grupos, tanto finitos como infinitos.

En general los grupos infinitos considerados en criptografía son finitamente presentados, es decir admiten un conjunto de generadores finito que satisfacen un conjunto finito de relaciones. Los esquemas propuestos se basan en la conocida dificultad de dos problemas, el de la palabra (¿podemos determinar si una palabra en los generadores representa o no el elemento identidad en el grupo?) y el de la conjugación (determinar si dos elementos del grupo son o no conjugados en el grupo).

En el caso de grupos finitos en general las propuestas se basan en la existencia de ciertos conjuntos, con propiedades especiales, que permiten escribir todos los elementos del grupo como producto de elementos de dichos conjuntos (como signaturas logarítmicas, mallas o cubiertas, ver [15]).

También se han utilizado grupos Braid en criptografía, si bien los esquemas diseñados han sido criptoanalizados en la mayoría de los casos.

Finalmente, en este sentido, comentemos que la primera propuesta de diseño para un criptosistema IND-CCA (que se ha convertido actualmente en la noción standard de seguridad deseable), se debe a Cramer y Shoup tomando como base grupos abelianos. También se han presentado propuestas basadas en grupos no abelianos (ver [16]).

5. Criptoanálisis

Las exigencias de seguridad han ido cambiando, dependiendo de necesidades y del perfeccionamiento y la sistematización lograda por el criptoanálisis. Se han desarrollado diversas nociones de seguridad, siendo este un campo teórico de trabajo en el que aún queda mucho por hacer. La noción de seguridad considerada depende de la cantidad de información conocida por un adversario y el tipo de ataques que pueda llevar a cabo. En algunos casos el adversario conoce pares de texto y sus cifrados, pero en otros casos puede ob-

tener el cifrado de cualquier mensaje previamente elegido, como ocurre en la criptografía de clave pública. Tambien puede ocurrir que cuando el atacante trata de recuperar un mensaje concreto *m* a partir de su cifrado *c*, tenga acceso al descifrado de cualquier otro texto cifrado.

El criptoanálisis y la criptografía van íntimamente ligados. Antes de proponer un sitema de cifrado, es necesario hacer una tarea de criptoanálisis, para tener una mínima seguridad de la robustez del esquema. El criptoanalista, en su tarea de buscar vulnerabilidades de los esquemas propuestos, utiliza gran variedad de herramientas matemáticas: técnicas estadísticas, algebraicas, algoritmos de optimización, teoría de números, etc. Una de las técnicas más potentes utilizadas por el criptoanálisis está basada en retículos.

Un retículo es el conjunto de combinaciones lineales enteras de un conjunto de vectores linealmente independientes (su estructura en dimensión 2 ó 3 se parece a una red). Estas estructuras tienen aplicaciones en otras partes de las matemáticas, como álgebras de Lie, en teoría de códigos correctores o en otras ciencias, como la cristalografía.

Las aplicaciones a criptología se hacen a través de la resolución de ciertos problemas como el del vector más corto. La complejidad de los mejores algoritmos conocidos para resolverlos crecen, al menos en el peor de los casos, exponencialmente con la dimensión del retículo.

Sin embargo A. J. Lenstra, H. W. Lenstra y L. Lovász vieron que si se quiere encontrar un vector *relativamente corto,* el problema es mucho más fácil y diseñaron un algoritmo, el LLL, que lo resuelve en un tiempo de ejecución que es polinomial en la dimensión del retículo.

El algoritmo LLL se utilizó en el problema de la mochila y en el criptoanálisis al sistema mencionado propuesto por Merkle y Hellman y también para probar la debilidad de algunas funciones hash (que juegan un importante papel en criptografía) o la vulnerabilidad de algunos generadores pseudoaleatorios de números.

Aunque la aplicación más espectacular de los retículos ha sido en criptoanálisis, también se han aplicado en criptografía. Ajtai y Dwork propusieron un criptosistema de clave pública basado en una variante, tambien difícil, del problema del vector más corto y además la seguridad se basaba en la difícultad de resolver el problema en un caso cualquiera, no en uno especialmente desfavorable. Pero si el tamaño de las claves es grande, el criptosistema es ineficiente y si se reducen las claves, el criptosistema es, a pesar de todo, vulnerable.

Goldwaser, Goldreich y Halevi propusieron otro criptosistema de clave pública cuya seguridad dependia de otro problema difícil, el encontrar el vector de un reticulo más cercano a otro vector dado. Este algoritmo es más eficiente que el de Ajtai y Dwork, pero la forma especial de los retículos utilizados los hace vulnerables ante un cierto tipo de ataques.

En la actualidad sólo existe un criptosistema de clave pública en uso que se basa en retículos, si bien no en su descripción inicial. El ataque más fuerte conocido se basa en resolver el problema del vector más corto en un retículo que se construye a partir de la clave pública y que no consigue resolverse porque se pueden utilizar dimensiones grandes debido a la eficiencia del sistema. Hay que hacer notar, sin embargo, que no hay ninguna demostración de que atacar al sistema pase necesariamente por resolver el problema del vector más corto.

Coppersmith realizó un significativo avance en el campo del criptoanálisis al publicar en 1996 unos algoritmos basados en retículos que permitian encontrar, con complejidad polinómica, soluciones pequeñas de ecuaciones enteras. Una versión modificada y más operativa dada por Howgrave-Graham permitió encontrar soluciones pequeñas de ecuaciones modulares. El diseño por parte de Boneh y Durfee de un algoritmo para atacar el RSA cuando la clave privada se escoge demasiado pequeña ha sido, probablemente, la aplicación más importante.

Finalmente notemos que en ocasiones herramientas del criptoanáliss se utilizan para probar la seguridad de un sistema criptográfico. Es el caso de un algoritmo de Coppersmith que busca raíces pequeñas de ecuaciones enteras en dos variables y que fue utilizado por May para probar que, en ciertas condiciones, la seguridad del RSA es equivalente al problema de la factorización.

6. Conclusiones

No se debe deducir de lo anterior, que la criptología se reduce al diseño de criptosistemas y al posterior estudio de sus debilidades en el criptoanálisis. Los problemas de los que se ocupa la criptografía son muy numerosos y no podríamos enumerarlos en estas páginas. Aparte del uso de passwords, ya generalizado, y todo lo que rodea al comercio y dinero electrónico, mencionaremos, a modo de ejemplo, sólo algunos de ellos:

1. *Autenticación de mensaje y firma digital:* Se trata de una de las principales aplicaciones de la criptografía de clave pública, aunque en muchas ocasiones se combine con clave privada. La firma digital, a diferencia de la manuscrita, garantiza no sólo que el emisor es quien afirma ser, sino que el mensaje llega a su destinatario sin alteraciones o modificaciones en el mismo.
2. *Compartición de secretos:* Se quiere dar información a un grupo de gente de modo que una información secreta sea recuperada si cualquier subconjunto de k personas colabora, pero no se consiga si son sólamente $k - 1$ los que colaboran.
3. *Acuerdo de bit:* Reproduce el proceso de lanzamiento de una moneda entre dos personas que están a distancia y tienen que interactuar de modo secuencial y no en el mismo instante.
4. *Pruebas de conocimiento cero y transferencia olvidadiza (oblivious transfer):* Se utiliza cuando una persona quiere convencer a otra de que posee una información o es capaz de hacer algo (por ejemplo demostrar un teorema) sin revelar los detalles. Un modo de construir pruebas de conocimiento cero no interactivas es a través de un canal de transferencia olvidadiza, que es un sistema para enviar dos paquetes de información cifrada sabiendo emisor y receptor que sólo uno de los dos paquetes puede ser descifrado y leido por el receptor y el emisor ignora cual de los dos paquetes será el que puede leer el receptor.

A los anteriores problemas podemos añadir el descubrimiento parcial de secretos, la venta de secretos, esquema electoral, transferencia inconsciente, firma de contratos, correo con acuse de recibo, etc. Como vemos la lista se prolonga de un modo realmente impresionante y la actividad en el campo es incesante. Basta echar un vistazo a las actas de alguna de las importantes reuniones que se celebran anualmente en el ámbito internacional, por ejemplo las del último Eurocyrpt en San Petersburgo (el de este año será en Barcelona) o a las de TCC 2007 (Theory of Cryptography Conference) que se celebrará este febrero en Amsterdam para ver la cantidad de investigación que se está realizando.

Hemos tratado de reflejar como distintas partes de las Matemáticas han jugado y están llamadas a jugar un papel esencial en el desarrollo de la Criptografia, especialmente en Clave Pública. Por supuesto la seguridad de la información necesita profesionales de muchos ámbitos, y muy especialmente informáticos. Shafi Goldwasser publicó un artículo en los Proceedings del IEEE en 1997 con el título: "Nuevas direcciones en Criptografía, Veinte años más tarde", en alusión a los 20 años transcurridos desde la introducción de la Criptografía de clave pública. El subtítulo de dicho artículo es "Criptografía y Teoría de la Complejidad: un emparejamiento hecho en el cielo". Esta idea aparece también expresada por Koblitz, que plantea la importancia de propuestas en criptografía, aunque no sean prácticas ni aplicables eventualmente. Las cuatro razones esgrimidas para ello son:

1. Pueden dar origen a nuevas cuestiones matemáticas o generar nuevos puntos de vista sobre teorías anteriores.
2. Pueden sugerir nuevas líneas de investigación en aspectos teóricos de Ciencias de la Computación y arrojar luz sobre las interrelaciones entre clases de complejidad.
3. Pueden ser un medio de popularizar matemáticas y Ciencias de la computación.
4. Pueden ser un medio efectivo para la enseñanza a niveles no-universitarios.

Por tanto los matemáticos han jugado y están llamados a jugar un importante papel en la seguridad de la información. Y al mismo tiempo, la fructífera relación con Ciencias de la Computación debe ser cuidada, mantenida y estimulada.

ARBOR CLXXXIII 725 mayo-junio [2007] 419-425 ISSN: 0210-1963

Referencias

[1] M. Ajtai y C. Dwork, A public-key cryptosystem with worst-case/ average case equivalente. *Proc. of 29th STOC, ACM.* 1997, 284-293.

[2] M. Bellare, A. Desai, D. Pointcheval y P. Rogaway, Relations Among Notions of Security for Public-Key Encryption Schemes *Proc. of CRYPTO '98, LNCS 1462,* 1998, 26-45.

[3] D. Boneh y G. Durfee, Cryptanalysis of RSA with private key less than $n^{0,292}$, *Proc. of Eurcrypt'99, Lecture Notes in Computer Science 8494*, 1999, 1-11.

[4] I. Cascudo, Aplicaciones de Retículos en Criptología. *Tesina de Licenciatura, Universidad de Oviedo,* 2006.

[5] D. Copperstmith, Small solutions to polynomial equations and low exponent RSA vulnerabilities. *Journal o f Cryptology 10(4),* 1997, 233-260.

[6] D. Copperstmith, Finding small solutions to small degree polynomials. *Proc. of Cryptography and Lattices Conference'01, Lecture Notes in Computer Science 2146,* 2001.

[7] D. Copperstmith y A. Shamir, Lattice attacks on NTRU. *Proc. of Eurocrypt'97, Lecture Notes in Computer Science 1238,* 1997, 52-61.

[8] R. Cramer y V. Shoup, A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack *Proc. of CRYPTO'98. LNCS, vol. 1162.,* 1999, 13-25.

[9] R. Cramer y V. Shoup, Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption *Cryptology e Print Archive: Report 2001/085,* 2001, 1-62.

[10] W. Diffie y M. E. Hellman, New directions in Cryptology. *IEEE Trans. Information Theory 22,* 1976, 644-654.

[11] O. Goldreich, S. Goldwasser y S. Halevi, Public-key cryptosystems from lattice reduction problems. *Proc. of Crypto'97, Lecture Notes in COmputer Science 1294,* 1997, 112-131.

[12] O. Goldreich. S. Goldwasser y S. Halevi, On the limits of non-approximitability of lattice problems. *Proc. of 80th STOC, ACM,* 1998.

[13] S. Golwasser, New directions in Cryptography: Twenty some years latter (or a Match Made in Heaven), *Proc. o f the 88th Annual IEEE Symposium on Foundations of Competer Science, FOCS'97,* 1997, 314-324.

[14] S. González, M. I. González-Vasco y C. Martínez, Esquemas de cifrado basados en grupos: pasado y futuro CD: *Tendencias actuales en la Criptología, Sesión especial de MAT.es 2005* ISBN: 84-689-0117-2.

[15] M. I. González-Vasco. Criptosistemas basados en Teoría de grupos. *Tesis Doctoral, Universidad de Oviedo,* 2000.

[16] M. I. González Vasco, C. Martínez, R. Steinwandt y J. L. Villar, A new CramerShoup like methodology for group based probably secure schemes. *Lecture Notes in Computer Science, Theory of Cryptography 3378,* 2005, 495-509.

[17] A. J. Lenstra, H.W. Lenstra y L. Lovász, Factoring polynomials with rational coefficients. *Mathematische Annalen 261.* 1982, 513-534.

[18] N. Koblitz, *Adgebraic Aspects of Cryptography,* Springer 2004.

[19] R. Merkle y M. Hellman, Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions of Information Theory, IT-24(5),* 1978, 525-530.

[20] P. Q. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem. *Lecture Notes in Computer Science 1666,* 1999, 288-304.

[21] P. Q. Nguyen y J. Stern, Lattice reduction in cryptology: An update. *Lecture Notes ira COmputer Science 1838,* 2000, 85-112.

[22] P. Q. Nguyen y J. Stern, The two faces of lattice in cryptography. *Lecture Notes in Computer Science 2146,* 2001.

[23] C. E. Shannon, Communication theory of secrecy systems, *Bell Syst. Tech. J. 18,* 1949, 656-715.

Recibido: 15 de enero de 2007
Aceptado: 25 de enero de 2007